Innovation Lab

Price Stability: Building crypto-finance innovation with Stablecoins

This paper describes “stablecoins” and different approaches to achieving market price stability of an independently issued token with a target currency.

Stablecoins represent an evolutionary step in the digitalization of commerce. Software developers rely on modular abstractions to create solutions. Blockchain technology has produced a number of innovative building blocks known as open finance “primitives”. They are critical building components in the developing crypto-financial ecosystem and move the space forward, enabling new and exciting crypto systems to move in-step with the non-crypto economy.

These components form psychological and technical bridges from the physical, legacy financial system to crypto, digital systems. Market price stability is a fundamental core financial primitive that many other use cases will build upon, such as payments, lending, collateralization, hedging and insurance, to name a few.

What are Stablecoins?

A physical coin is a representation of physical scarcity and authenticity. It also embodies a type of security: if you have the coin, I don’t have it anymore. This is the primordial sacrifice of exchange. The coin is a token which enforces physical-world accounting rules.

Representing balances digitally presents a dilemma because we do not have the physical scarcity to enforce these accounting rules. Moving from atoms to bits has many advantages, but we lose the convenience and simplicity of physical scarcity as accounting enforcement.

A solution to the digital double-spend problem is one of the major benefits of blockchain technology. But cryptocurrency tokens or coins currently have developed a different

market-oriented problem. Because they are poorly understood, regulation is shifting and inconsistent, adoption is nascent, markets are thinly traded, and large holders can potentially manipulate prices - they exhibit volatility which acts as a hindrance to use. A seller of goods or services cannot justify the costs of updating prices or of bearing the risks of not doing so.

So how can we create a medium of exchange that can take advantage of the digital infrastructure and significant practical benefits of blockchain technology, but without the market price volatility associated with non-sovereign cryptocurrencies?

Stablecoins seek to accomplish just that. They seek to closely target the tradable value of a specific sovereign currency, e.g. 1 USDC = 1 USD. That sounds easy enough on the surface, but the FED or SNB is not (yet) the issuer of these stablecoins and the market is a harsh mistress.

> *The goal of stablecoins is to get the blockchain medium of exchange benefits without the cryptocurrency store of value drawbacks.*

Fiat Collateral Stablecoins

Sometimes troubled sovereign states seek stability in their currency relative to a dominant, larger currency through the use of a currency “peg”. The most common peg mechanism is where a country’s central bank establishes a fixed exchange rate by promising to freely exchange their currency for the peg target currency at the fixed rate. This means, however, that the central bank in question must have a sufficient supply of the peg target currency to satisfy exchange demand, at least until confidence is established: the success and longevity of any peg rises and falls with the confidence of this promise.

Predictable redeemability is a straightforward (if not primitive) mechanism to achieve market price stability in a stablecoin. An issuer of such a stable coin must provide some credible proof that the redeemable collateral exists to garner the confidence required to sustain a stable value.

Here is where issues arise. The real-world fiat collateral must be safely held. An independent custodian is the obvious choice but is accompanied by costs. Also, transparency is only vaguely offered periodically and auditors (further costs) attest the balances. Intra-period, one must simply hope that the funds exist. These stablecoins are

centralized due not only to the fact that a centralized counterparty holds the collateral, but also in the fact that regulators require certain superpowers be embedded in the token contract code and granted to the issuer. This means the issuer will have some ability to seize/confiscate/freeze/reverse/censor funds or transactions should they choose or be compelled to. Here is an example of the centralized permissions in the USDC code:

```
157     /**
158      * @dev Adds account to blacklist
159      * @param _account The address to blacklist
160      */
161     function blacklist(address _account) public onlyBlacklister {
162         blacklisted[_account] = true;
163         emit Blacklisted(_account);
164     }
```

```
244   /**
245    * @dev called by the owner to pause, triggers stopped state
246    */
247   function pause() onlyPauser public {
248     paused = true;
249     emit Pause();
```

Or here in TUSD:

```
1091    // Destroy the tokens owned by a blacklisted account
1092    function wipeBlacklistedAccount(address _account) public onlyOwner {
1093        require(_isBlacklisted(_account), "_account is not blacklisted");
1094        uint256 oldValue = _getBalance(_account);
1095        _setBalance(_account, 0);
1096        totalSupply_ = totalSupply_.sub(oldValue);
1097        emit WipeBlacklistedAccount(_account, oldValue);
1098        emit Transfer(_account, address(0), oldValue);
1099    }
```

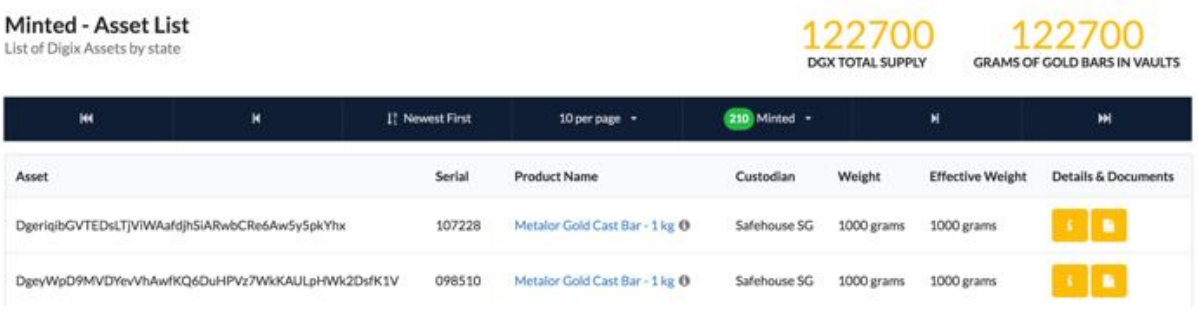
Or here in USTD:

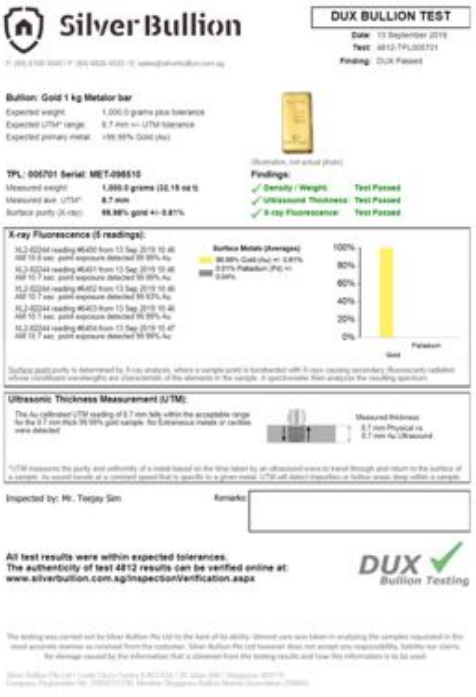
```
291     function destroyBlackFunds (address _blackListedUser) public onlyOwner {
292         require(isBlackListed[_blackListedUser]);
293         uint dirtyFunds = balanceOf(_blackListedUser);
294         balances[_blackListedUser] = 0;
295         _totalSupply -= dirtyFunds;
296         DestroyedBlackFunds(_blackListedUser, dirtyFunds);
297     }
```

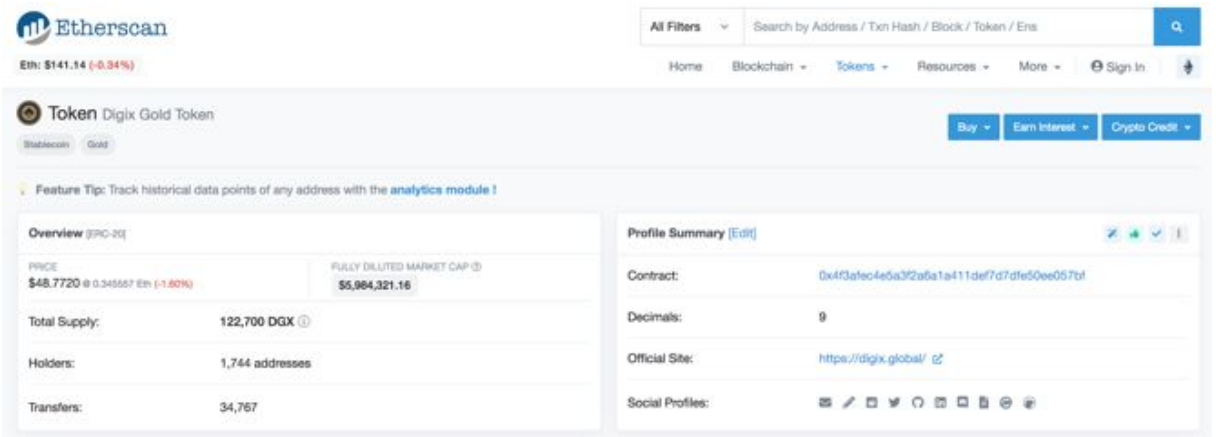
Commodity Collateral Stablecoins

Another caveat to the fiat-collateralized stablecoins is the current environment of negative interest rates. Swiss Crypto Tokens (Bitcoin Suisse), the issuer of XCHF, a Swiss Franc stablecoin creates a rolling, one-month bond and uses vault cash to avoid negative rates imposed by the Swiss National Bank.

Another category of stablecoin uses the physical commodity as the underlying collateral. The company Digix Global has created a similar setup for the stablecoin (DGX) representing one gram of gold. Again, physical gold is stored at a 1:1 ratio, backing the tokens minted (a common term for token creation which increments the token supply). They maintain a sophisticated process for minting, storing and documenting the gold in their vaults. The tokens are redeemable for physical gold (101 DGX minimum for a certified 100-gram ingot).







Crypto Collateral Stablecoins

A third category of stablecoin tries to create stable market price valuation by collateralizing cryptocurrency. But the underlying collateral is not the value being pegged. Because the underlying cryptocurrency value is different and volatile, the stablecoin's collateral value must be overcollateralized to ensure reliable backing of value even when the collateral value experiences significant price swings.

The most prominent example is the Maker Foundation's DAI, which is collateralized by a basket of underlying cryptocurrencies. It is known as Multi-collateral DAI and targets price parity with USD.

DAI Mechanics

In contrast with fiat- or commodity-collateralized stablecoins, cryptocurrency collateralized stablecoins hold the collateral on the blockchain in smart contracts. This is a significant change and benefit over the latter. It means that anyone can inspect and verify the real-time state of the collateral account, enabling ad-hoc audit of the entire system. It also means that custodial counterparty risk and costs are obviated.

The Maker smart contract system creates stability by securing collateral, enabling different participants with tools and economic incentives.

As the market shifts the DAI demand curve due to external factors like expectations, confidence or adoption, the price will vary from 1.0 DAI/USD. The DAI smart contract system strives to move the equilibrium price back to 1.0 by adjusting the DAI supply through various mechanisms.

Normal users of DAI will usually buy these tokens on an exchange. But users can also create their own DAI, by locking ETH (the native token of the Ethereum blockchain) or other designated Ethereum-based tokens in a smart contract called a Vault. The current minimum collateralization ratio is 150%, meaning that ETH in the value of USD 150 locked in a Vault will create DAI 100 from which the user can draw. The user can transfer and spend these DAI tokens arbitrarily, but their ETH remains locked in the Vault as collateral. Only the return of 100 DAI can fully free the ETH in their Vault.

In this example where the collateralization ratio is at the minimum, any price decline in ETH will trigger liquidation of the Vault. When a Vault is liquidated, the Maker smart contract system autonomously initiates a Collateral Auction where Vault's ETH is auctioned off for DAI to the point where the minimum collateralization ratio is again achieved. Vault owners can increase the safety of their Vaults by returning DAI to the Vault or conversely, adding more ETH. For example, generating only 50 DAI from the Vault above would leave it with a collateralization ratio of 300%. The market price of ETH could drop 50% before the Vault is in danger of liquidation.

Vault creators must pay a Stability Fee. This is currently 6% p.a. and is paid automatically when the Vault is extinguished. Should a liquidation be triggered by falling ETH price, a liquidation penalty of 13% is paid out of any ETH remaining post-liquidation.

Returning the same amount of DAI that was minted allows the Vault creator to release all ETH collateral. The DAI are burned (a common term for destroying tokens and provably removing them from supply) by the Maker smart contract system, reducing the total DAI supply.

Essentially, the DAI maintains USD price parity through an intricate system composed of collateral (Vault Positions), autonomous smart contract feedback mechanisms and economically incentivized external participants.

DAI Savings Rate

A further lever on DAI total supply recently introduced to the Maker smart contract system is the DAI Savings Rate or DSR. This is an interest rate which is earned when users send DAI to the DSR contract, locking the DAI and effectively removing it from circulation. The DSR is a mechanism which can also impact DAI total supply and circulation. Higher interest rates will incentivize DAI to be locked, but also DAI creation and increased collateral levels. Currently the DSR is 6%, which is the same rate as the Stability Fee.

Price Oracles

Blockchain systems have no native means to interface with the real world and cannot know about exogenous events or data on their own. As such, they must rely on “Oracles” to inject the external data that smart contracts might require.

To facilitate stability, the Maker smart contract system must have information on the current market prices of the different collateral types fed to it. Clearly, this is an extremely sensitive area for the system as it will autonomously react and trigger events and actors depending on the price data delivered by the Oracles. The Maker smart contract system mitigates Oracle risk by specifying multiple addresses that are whitelisted for each collateral type. The median price across all Oracles is selected (to prevent outlier skew) and the price is effective with a 1-hour delay to grant the Maker governance community a reaction window.

Decentralized

There are no restrictions on how DAI is used or integrated. DAI endeavors to be decentralized and has no pause, freeze or blacklist capabilities. An Emergency Shutdown Module does, however exist. The consequences of an Emergency Shutdown are a global system freeze and the ability to redeem collateral at respective market prices at the time of

shutdown by DAI holders. The Emergency Shutdown is intended to mitigate malicious governance and prevent exploits of critical vulnerabilities.

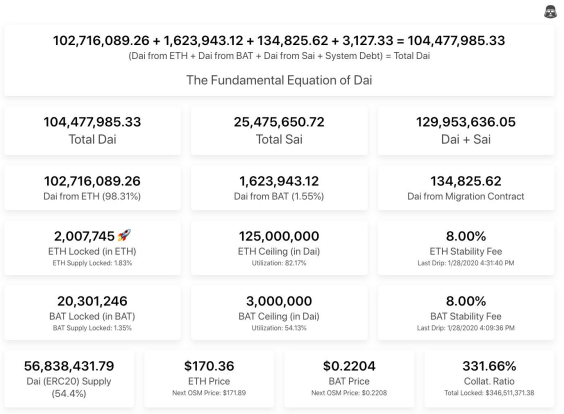
The Maker system configuration is steered through the MKR token used in governance votes. These votes impact certain key configuration parameters in the Maker system such as collateral ceiling or the DSR. Governance votes are taken here and all MKR token holders can participate:

Vote.makerdao.com

These changes affect the Maker system immediately. The votes and parameters can be transparently verified. These independent websites offer a view into the on-chain state of the Maker system:

Makerburn.com

daistats.com



Conclusion

Stablecoins help participants in the digital economy transition to cryptographically secure money with all the benefits of blockchain technology, but without the uncertainty about the future value of their tokens. Systems and applications can freely integrate digital money without restrictions or volatility, benefitting from the transparent, open, real-time and verifiable nature of these decentralized digital currencies.

About us

The i.AM Innovation Lab develops innovative business models and creates mobile & web applications for investment & asset managers.

We foster collaboration in the asset management industry by creating joint initiatives & solutions.

Would you like to discuss this or any other subject?

Please write us an email or visit us.

John Orthwein
Technology & Decentralized Finance
john.orthwein@iam-lab.ch

Claudio Schneider
Co-Founder & Partner
claudio.schneider@iam-lab.ch

iAM Innovation Lab